RÉPUBLIQUE FRANÇAISE PCT/ 03/00946

03 Str

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

REC'D 10 APR 2003
WIPO PCT

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 03 MARS 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE
page 1/2

R1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /300301

Réservé à l'INPI

REMISE DES PIÈCES
DATE 7 MARS 2002
LIEU 75 INPI PARIS B
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0202918
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI - 7 MARS 2002

Vos références pour ce dossier (facultatif) FR 76.0728/PR

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CP8
RENAULT Patricia -
36-38, rue de la Princesse
BP 45
78431 LOUVECIENNES CEDEX

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — Cochez l'une des 4 cases suivantes

Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A CLE SECRETE.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR ☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**

Nom ou dénomination sociale		CP8
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		3 2 9 5 5 6 1 4 6
Code APE-NAF		8 3 2
Adresse	Rue	36 – 38 rue de la Princesse – BP 45
	Code postal et ville	7 8 4 3 1 LOUVECIENNES CEDEX
	Pays	France
Nationalité		Française
N° de téléphone (facultatif)		01.30.08.48.33
N° de télécopie (facultatif)		01.30.08.45. 22
Adresse électronique (facultatif)		PATRICIA.RENAULT@LOUVECIENNES.SEMA.SLB.COM

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

R2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 7 MARS 2002
LIEU 75 INPI PARIS B
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0202918

DB 540 W / 030301

Vos références pour ce dossier : *(facultatif)*	**FR 76.0728/PR**
6 MANDATAIRE	
Nom	RENAULT
Prénom	Patricia
Cabinet ou Société	CP8
N °de pouvoir permanent et/ou de lien contractuel	PG 10297
Adresse — Rue	36 – 38 rue de la Princesse – BP 45
Adresse — Code postal et ville	7 8 4 3 1 LOUVECIENNES CEDEX
N° de téléphone *(facultatif)*	01.30.08.48.33
N° de télécopie *(facultatif)*	01.30.08.45.22
Adresse électronique *(facultatif)*	PATRICIA.RENAULT@LOUVECIENNES.SEMA.SLB.COM
7 INVENTEUR (S)	
Les inventeurs sont les demandeurs	☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE	**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé	☒ ☐
Paiement échelonné de la redevance	**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES	**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes	0

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)

RENAULT Patricia
Mandataire

VISA DE LA PRÉFECTURE OU DE L'INPI

M. BLANCANEAUX

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A CLE SECRETE

La présente invention concerne un procédé de sécurisation d'un ensemble électronique mettant en œuvre un algorithme cryptographique qui utilise une clé secrète. Plus précisément, le procédé vise à réaliser une version de l'algorithme qui ne soit pas vulnérable face à un certain type d'attaques physiques – dites *High-Order Differential Power Analysis* - qui cherchent à obtenir des informations sur la clé secrète à partir de l'étude de la consommation électrique de l'ensemble électronique au cours de l'exécution du calcul.

DOMAINE TECHNIQUE

Les algorithmes cryptographiques considérés ici utilisent une clé secrète pour calculer une information de sortie en fonction d'une information d'entrée ; il peut s'agir d'une opération de chiffrement, de déchiffrement ou de signature ou de vérification de signature, ou d'authentification ou de non-répudiation. Ils sont construits de manière à ce qu'un attaquant, connaissant les entrées et les sorties, ne puisse en pratique déduire aucune information sur la clé secrète elle-même.

On s'intéresse donc à une classe plus large que celle traditionnellement désignée par l'expression *algorithmes à clé secrète* ou *algorithmes symétriques*. En particulier, tout ce qui est décrit dans la présente demande de brevet s'applique également aux algorithmes dits à clé publique ou algorithmes asymétriques, qui comportent en fait deux clés : l'une publique, et l'autre, privée, non divulguée, cette dernière étant celle visée par les attaques décrites ci-dessous.

Les attaques de type Analyse de Puissance Electrique, *Power Analysis* en langage anglo-saxon, partent de la constatation qu'en réalité l'attaquant peut acquérir des informations, autres que la simple donnée des entrées et des sorties, lors de l'exécution du calcul, comme par exemple la

consommation électrique du microcontrôleur ou le rayonnement électromagnétique émis par le circuit.

L'analyse de consommation électrique différentielle constitue le principe d'une classe d'attaques, dites *Differential Power Analysis* en langage anglo-saxon, en abrégé DPA, permettant d'obtenir des informations sur la clé secrète contenue dans l'ensemble électronique, en effectuant une analyse statistique des enregistrements de consommation électrique effectués sur un grand nombre de calculs avec cette même clé.

Dans la plus simple de ces attaques, dite « DPA d'ordre 1 » ou simplement « DPA » quand il n'y a pas de risque de confusion, l'attaquant enregistre les signaux de consommation de courant et calcule des propriétés statistiques individuelles du signal à chaque instant. On considère ici les attaques dites Analyse de consommation électrique différentielle d'ordre supérieur, *High-Order Differential Power Analysis* en langage anglo-saxon, en abrégé HO-DPA, qui généralisent l'attaque « DPA d'ordre 1 » : l'attaquant calcule maintenant des propriétés statistiques conjointe de la consommation électrique considérée à plusieurs instants différents. Plus précisément une attaque « DPA d'ordre n » prend en compte n valeurs du signal de consommation, qui correspondent à n valeurs intermédiaires différentes apparaissant au cours du calcul de l'algorithme cryptographique. Les valeurs intermédiaires détectées par les attaques seront appelées dans ce qui suit, informations critiques.

On considère, à titre d'exemple non limitatif, le cas de l'algorithme DES (*Data Encryption Standard*), dont on peut trouver une description dans FIPS PUB 46-2, *Data Encryption Standard*, 1994, document indiqué à titre de référence.

L'algorithme DES se déroule en 16 étapes appelées tours (voir figure 2). Dans chacun des 16 tours, une transformation f est effectuée sur 32 bits. Cette transformation f utilise huit transformations non linéaires de 6 bits sur 4 bits, qui sont codées chacune dans une table appelée boîte-S (S sur la figure 2).

Une attaque « DPA d'ordre 2 » sur le DES peut être mise en

œuvre de la manière suivante :

Dans une première étape, on fait des mesures de consommation sur le premier tour, ceci pour 1000 calculs de DES. On note E[1], ..., E[1000] les valeurs d'entrée de ces 1000 calculs. On note C[1], ..., C[1000] les 1000 courbes correspondantes de consommation électrique mesurées lors de ces calculs.

Dans une deuxième étape, supposons que deux bits (constituant des informations critiques), de valeurs respectives b_1 et b_2, apparaissent au cours du calcul et sont tels que $b_1 \oplus b_2$ soit égal à la valeur b du premier bit de sortie de la première boîte-S lors du premier tour. Ici $\oplus$ désigne la fonction "OU-exclusif" bit à bit. On fait une hypothèse sur l'intervalle de temps δ entre l'instant où se trouve le point de la courbe de consommation correspondant à b_1 et celui correspondant à b_2. On associe alors à chaque courbe C[i], où i est un entier prenant successivement les valeurs 1, 2, ..., 1000, une autre courbe $C_\delta[i]$, égale à la différence entre C[i] et la courbe obtenue à partir de C[i] par translation d'une valeur δ suivant l'axe des abscisses. On calcule également la courbe moyenne CM des 1000 courbes $C_\delta[i]$.

Dans une troisième étape, il est facile de voir que b ne dépend que de 6 bits de la clé secrète. L'attaquant fait une hypothèse sur les 6 bits concernés. Il calcule – à partir de ces 6 bits et des E[i] – les valeurs théoriques attendues pour b. Cela permet de séparer les 1000 entrées E[1], ..., E[1000] en deux catégories : celles qui donnent b=0, et celles qui donnent b=1.

Dans une quatrième étape, on calcule maintenant la moyenne CM' (respectivement CM") des courbes $C_\delta[i]$ correspondant à des entrées de la première catégorie (respectivement de la deuxième catégorie), c'est-à-dire pour lesquelles b=0 (respectivement b=1). Si CM' et CM" présentent une différence notable, on considère que les valeurs retenues pour les 6 bits de clé, ainsi que le choix de la valeur δ étaient les bons. Si CM' et CM" ne présentent pas de différence sensible, au sens statistique, c'est-à-dire pas

de différence nettement supérieure à l'écart type du bruit mesuré, on recommence la 2ème étape avec un autre choix pour les 6 bits. Si aucun choix des 6 bits de clé n'est concluant, on recommence les étapes 3 et 4 avec un autre choix de δ.

Dans une cinquième étape, on répète les étapes 2, 3 et 4 avec deux bits dont le « ou-exclusif » est issu de la deuxième boîte-S, puis de la troisième boîte-S, ..., jusqu'à la huitième boîte-S. On obtient donc finalement 48 bits de la clé secrète.

Dans une sixième étape, les 8 bits restants peuvent être trouvés par recherche exhaustive.

En théorie, la DPA d'ordre n ne nécessite aucune connaissance sur la consommation électrique individuelle de chaque instruction, ni sur la position dans le temps de chacune de ces instructions. Elle s'applique de la même manière si on suppose que l'attaquant connaît des sorties de l'algorithme et les courbes de consommation correspondantes. Elle repose uniquement sur l'hypothèse fondamentale selon laquelle :

Il existe un ensemble de n variables intermédiaires, apparaissant dans le cours du calcul de l'algorithme, telle que la connaissance de quelques bits de clé, en pratique moins de 32 bits, permet de décider si deux entrées, respectivement deux sorties, donnent ou non la même valeur pour une fonction connue de ces n variables.

Tous les algorithmes utilisant des boîtes-S, tels le DES, sont potentiellement vulnérables à la « High Order DPA », car les modes de réalisation usuels, y compris ceux conçus pour résister aux attaques « DPA d'ordre 1 », restent en général dans le cadre de l'hypothèse mentionnée ci-dessus.

En pratique, la mise en place nécessite également de trouver (par recherche exhaustive ou par la connaissance d'autres informations, par exemple le détail de l'implémentation de l'algorithme cryptographique) les intervalles de temps entre les points de la courbe de consommation correspondant aux n variables considérées.

Un but de la présente invention est de supprimer des risques d'attaques « DPA d'ordre n », pour toutes les valeurs de n, d'ensembles ou systèmes électroniques de cryptographie à clé secrète ou privée.

Un autre but de la présente invention est d'offrir une protection des systèmes électroniques de cryptographie telle que l'hypothèse fondamentale précitée ne soit plus vérifiée, à savoir qu'aucune fonction connue d'un ensemble de n variables intermédiaires ne dépende de la connaissance d'un sous-ensemble aisément accessible de la clé secrète ou privée, les attaques de « High Order DPA » étant ainsi rendues inopérantes.

RESUME DE L'INVENTION

La présente invention concerne un procédé de sécurisation d'un système électronique comprenant un processeur et une mémoire, mettant en œuvre un processus de calcul cryptographique stocké dans la mémoire qui utilise une clé secrète caractérisé en ce qu'il consiste à masquer des résultats intermédiaires en entrée ou en sortie d'au moins une fonction critique dudit processus exécuté au moyen du processeur.

DESCRIPTION SOMMAIRE DES DESSINS

D'autres buts, avantages et caractéristiques de l'invention apparaîtront à la lecture de la description qui va suivre de la mise en oeuvre du procédé selon l'invention et d'un mode de réalisation d'un système électronique adapté pour cette mise en œuvre, donnés à titre d'exemple non limitatif en référence aux dessins ci-annexés dans lesquels:

- les figures 1a et 1b montrent une représentation schématique de deux types de fonction de remplacement du procédé selon la présente invention ;
- la figure 2 montre une représentation schématique d'un tour de l'algorithme DES classique ;

- les figures 3a à 3e montrent une représentation schématique de chaque type de tour possible de l'algorithme DES auquel le procédé selon l'invention est appliqué ;
- la figure 4 est une représentation symbolique sous forme d'un automate de l'algorithme DES auquel le procédé selon l'invention est appliqué.

MANIERE DE REALISER L'INVENTION

Le procédé selon l'invention vise à sécuriser un système électronique, et par exemple un système embarqué tel qu'une carte à puce mettant en œuvre un processus de calcul cryptographique qui utilise une clé secrète. Le système électronique comprend un processeur et une mémoire. Le processus de calcul cryptographique est installé dans la mémoire, par exemple de type ROM dudit système. Le processeur dudit système exécute le processus de calcul en utilisant une clé secrète, stockée dans une zone secrète d'une mémoire, par exemple de type E2PROM.

Le procédé selon l'invention consiste à masquer des résultats intermédiaires constituant des informations critiques obtenues lors du processus de calcul en entrée ou en sortie d'une fonction, appelée ci-après fonction critique.

Le procédé remplace une fonction critique par une fonction de remplacement qui effectue le « même » calcul mais sur des données modifiées en entrée ou en sortie.

Comme montré sur les figures 1a et 1b, toute fonction f de n bits vers m bits effectuant un calcul (calcul par une succession d'opérations de base, par la consultation d'une table ...) est remplacée par une nouvelle fonction p qui sera la composée de f avec une autre fonction g (de n' bits vers n bits) (figure 1a) ou h (de m bits vers m' bits)(figure 1b), g étant

effectuée avant f et h après ; le procédé remplace donc dans le calcul f par (g -> f) ou par (f-> h).

Selon un exemple illustratif, g et h sont des opérations de masquage de données de la forme « ou exclusif ». La fonction p prend en entrée des données masquées par g ou ressort en sortie des données masquées par h.

Le terme « masquer » dans la présente description signifie transformer par une fonction non publique (interne, inconnue de l'utilisateur de la carte), par exemple une fonction utilisant un aléa.

Le masquage d'une première fonction critique d'un processus de calcul a lieu en sortie par une fonction h ; le masquage d'une dernière fonction critique d'un processus de calcul a lieu en entrée par une fonction g. De cette manière, le processus de calcul reçoit en entrée et donne en sortie des données non masquées : le masquage est transparent pour l'extérieur. Une personne souhaitant effectuer une attaque de type DPA sur le système ne sait pas que les résultats intermédiaires constituant des informations détectables sont masquées et ne pourra tirer aucune conclusion de ses résultats sans en comprendre la raison.

On notera bien, que la taille des données en entrée de g (et des données en sortie de h) ne seront pas forcément de la même taille que celles de f.

L'invention présente deux aspects : la transformation du processus de calcul lui-même (comment faire pour lui inclure une fonction modifiée) ainsi que le mode de calcul de la fonction modifiée (par exemple la méthode pour construire la nouvelle table s'il s'agissait à la base d'un accès à une table).

La description qui suit décrit une application de la présente invention à l'algorithme DES. Dans un premier temps, un premier exemple simplifié mais facilement compréhensible est présenté pour permettre dans un deuxième temps d'étudier divers développements qui découlent directement de ce premier exemple.

Le procédé selon la présente invention résoud deux problèmes de manière indépendante :

comment s'articule le DES utilisant des S-boites modifiées, et

la construction de ces S-boites.

L'articulation du DES en utilisant des boîtes-S modifiés dans un premier exemple simplifié est décrit dans ce qui suit par référence aux figures 2, 3a à 3e et 4.

On considère tout d'abord le $i^{ème}$ tour du DES (figure 2). Les S-boites du DES classique sont modifiées afin de manipuler des données masquées. On considère alors α une valeur quelconque de 32 bits. On définit deux nouvelles fonctions S'_1 et S'_2 de 48 bits vers 32 bits par :

$S'_1(x) = S(x \text{ xor } E(\alpha))$ pour tout x sur 32 bits

$S'_2(x) = S(x) \text{ xor } P^{-1}(\alpha)$ pour tout x sur 32 bits

On définit alors deux fonctions $f'_{1,Ki}$ et $f'_{2,Ki}$ analogues à la fonction f_{Ki} mais utilisant les boites S'_1 et S'_2 en lieu et place de S.

Les deux nouvelles fonctions permettent pour $f'_{1,KI}$ d'obtenir une valeur masquée par α à partir d'une valeur non masquée et inversement pour $f'_{2,KI}$.

Les figures 3a à 3e représente l'ensemble des schémas de tour de DES (A à E) obtenus en utilisant des valeurs masquées ou non par α et les différentes boites (S_{KI} , $S'_{1,Ki}$ ou $S'_{2,Ki}$). Par soucis de clarté, les données

masquées sont indiquées en traits pointillés alors que les données non masquées (normale) sont en traits pleins.

La figure 4 représente l'ensemble des enchaînements de tours susceptibles d'être obtenus symbolisé sous la forme d'un automate. Comme indiqué précédemment, pour partir et arriver à des données non masquées, les états de commencement sont A ou B alors que ceux de terminaisons sont A ou E.

Ainsi, il est possible d'effectuer un DES entier (à 16 tours) par l'enchaînement : IP – BCDCDCEBCDCDCDCE – IP^{-1}. A partir d'un message M, le procédé permet d'obtenir un chiffré habituel (celui qui aurait été obtenu avec l'enchaînement IP – AAAAAAAAAAAAAAAA – IP^{-1}), à savoir sans démasquage à l'entrée et en sortie.

Il existe de nombreuses combinaisons valides ; certaines permettent même de ne masquer que les premiers et les derniers tours en utilisant des tours normaux (de type A) entre ces tours masqués ; comme par exemple : IP – BCEAAAAAAAAAABCE – IP^{-1}.

Selon un développement de l'invention, les données sont masquées avec des masques différents suivant les tours. En prenant les notations de tours adoptés ci-dessus (A,B,C,D et E), on ajoute un index (α,β,γ ...) qui symbolise le masque de 32 bits utilisé pour le masquage. Ainsi on voit que le tour B de l'exemple simplifié ci-dessus s'écrit à présent B_α. Il est à noter que le tour A n'a pas besoin d'être indexé par une valeur de masque car le masque n'intervient pas. Dans cet exemple de généralisation, un DES s'effectue selon l'enchaînement suivant :

$$IP - B_\alpha C_\alpha D_\alpha C_\alpha D_\alpha C_\alpha E_\alpha B_\beta C_\beta D_\beta C_\beta D_\beta C_\beta D_\beta C_\beta E_\beta - IP^{-1}$$

De cette manière, les tours, et particulièrement les premiers et le dernier sensible aux attaques, sont protégés par des masques indépendants.

Pour effectuer les calculs précités, il est nécessaire de construire des S-Boites de type S, $S'_{1,\alpha}$, $S'_{2,\alpha}$,$S'_{1,\beta}$ et $S'_{2,\beta}$.

Les différentes S-Boites modifiées utilisées par le procédé selon la présente invention sont construites de manière sécurisée sur la base des formules suivantes :

$$S'_{1,\alpha}(x) = S(x \text{ xor } E(\alpha))$$
$$S'_{1,\beta}(x) = S(x \text{ xor } E(\beta))$$
$$S'_{2,\alpha}(x) = S(x) \text{ xor } P^{-1}(\alpha)$$
$$S'_{2,\beta}(x) = S(x) \text{ xor } P^{-1}(\beta)$$

Lesdites formules se décomposent suivant les opérations de bases énoncées ci-après :

Tirer une valeur aléatoire (comme α, β ...) ;

Permuter les bits d'une valeur secrète (comme E(α), $P^{-1}(\beta)$ ...) ;

Effectuer le XOR d'une valeur (comme $P^{-1}(\alpha)$ par exemple) avec un tableau de valeur correspondant aux valeurs habituelles de la S-Boite (en entrée ou en sortie).

Le tirage d'une valeur aléatoire de n bits (dans le cas du DES, n = 32) s'effectuent sur la base de l'algorithme suivant.

Le système dans lequel le procédé est mis en œuvre comprend un tableau « t » de n octets ainsi qu'une source d'aléas sur un octet notée « rand ». L'algorithme se déroule de la manière suivante :

Pour i allant de 0 à n-1 : t[i] := rand % 2

Pour i allant de 0 à m-1 : échanger t[rand % n] et t[rand % n]

Où m est un nombre à priori supérieur ou égal à n.

« % » représente l'opération modulo ou reste de la division entière.

Le résultat cherché est la concaténation des n bits contenus dans le tableau t.

Selon une première variante, le système comprend un tableau t de n / 4 octets.

Pour i allant de 0 à n/4 –1 : t[i] := rand
Pour i allant de 0 à m : Echanger t[rand % (n/4)] et t[rand % (n/4)]

Où m sera à priori supérieur à n/4.

Le résultat est la concaténation des quatre premiers bits de chacun des n/4 octets de t.

Selon une deuxième variante, on reprend l'algorithme selon la première variante en utilisant n/2, n/3, n/8 ou tout diviseur de n.

Selon une troisième variante, au lieu d'échanger des cases de manière aléatoire, on choisit une case aléatoirement et on lui ajoute par l'opération XOR une valeur aléatoire.

La permutation de n bits d'une valeur secrète vers m bits (dans le cas du DES : dans la permutation $P^{-1}(\beta)$: n = 48 et m = 32, dans la permutation $E(\alpha)$: n = m = 32) se base sur l'algorithme suivant.

Dans l'exemple décrit, on souhaite permuter un tableau noté « in » de n bits vers un tableau note « m » de m bits ; le système comprend un tableau « temp » de m valeurs (chaque case pouvant contenir la valeur n-1).

On construit dans le tableau temp une permutation des nombres

0,1,2, ... , m-2, m-1

Pour i allant de 0 à m-1 : out[V[temp[i]]] := in [temp[i]]

En fait, il s'agit d'effectuer une permutation de manière aléatoire bit par bit.

Selon une première variante, la permutation est réalisée non pas bit par bit mais k bits par k bits, le tout de manière aléatoire.

Selon une deuxième variante, on peut également ajouter à cela des valeurs fictives dans la table V, et/ou dans la table d'entrée et/ou de sortie. Ainsi si l'on utilise des octets pour stocker un bit, on peut compléter les autres bits « vacants » avec de l'aléas.

La réalisation de l'opération XOR consiste à ajouter une valeur (comme $P^{-1}(\alpha)$) de n bits à un tableau t de m valeurs.

L'opération peut être effectuée de manière aléatoire sur les octets du tableau de sortie ainsi que sur les bits de ces octets.

Selon une variante, on peut également ajouter des valeurs fictives tant dans les bits de α que dans le tableau t.

Le procédé selon l'invention utilise une fonction non publique de masquage lors de la construction des boîtes-S sans faire intervenir la clé. Lorsque le processus de calcul se déroule, aucun masque n'intervient. Ainsi, le procédé selon l'invention permet de sécuriser le système électronique contre toute attaque utilisant le masque même sans le connaître.

Il est à souligner que tout autre type de tirage et de permutation peuvent être utilisés pour la construction des boîtes-S modifiés.

De plus, la construction des boîtes-S basées sur les trois opérations décrites peut être réalisée sous tout autre type de forme et en particulier sous une autre forme qu'une boîte-S propre au DES utilisé comme exemple dans la présente description.

REVENDICATIONS

1-Procédé de sécurisation d'un système électronique mettant en œuvre un processus de calcul cryptographique qui utilise une clé secrète caractérisé en ce qu'il consiste à masquer des résultats intermédiaires en entrée ou en sortie d'au moins une fonction critique dudit processus.

2-Procédé selon la revendication 1, caractérisé en ce qu'il comprend une fonction de remplacement d'une fonction critique dudit processus effectuant le même calcul mais sur des résultats masqués en entrée ou en sortie.

3-Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il consiste à enchaîner des fonctions de remplacement de manière à fournir des résultats non masqués à l'entrée et en sortie dudit processus.

4-Procédé selon l'une des revendications 1 à 3, caractérisé en ce qu'il consiste à utiliser des masques différents suivant les fonctions critiques concernées.

5-Procédé selon la revendication 2, caractérisé en ce que la fonction de remplacement sur des résultats masqués en entrée est construite sur la base des opérations suivantes :

- une opération de masquage non publique ;
- une opération effectuant le même calcul que la fonction critique mais sur des résultats masqués par la fonction de masquage.

6-Procédé selon la revendication 2, caractérisé en ce que la fonction de remplacement sur des données masquées en sortie est construite sur la base des opérations suivantes :

- une opération effectuant le même calcul que la fonction

critique mais sur des résultats qui doivent être masquées par la fonction de masquage.

- une fonction de masquage non publique.

7-Procédé selon l'une des revendications 5 ou 6, caractérisé en ce qu'il consiste à enchaîner les opérations de la fonction de masquage de manière aléatoire.

8-Système électronique comprenant des moyens de mémorisation d'un processus de calcul cryptographique qui utilise une clé secrète, des moyens d'exécuter ledit processus de calcul caractérisé en ce qu'il comprend des moyens de masquage de résultats intermédiaires en entrée ou en sortie d'au moins une fonction critique dudit processus.

9-Système électronique selon la revendication 8, caractérisé en ce que les moyens de masquage des résultats intermédiaires et de calcul selon la fonction critique mais avec lesdits résultats masqués sont constitués par une boîte-S.

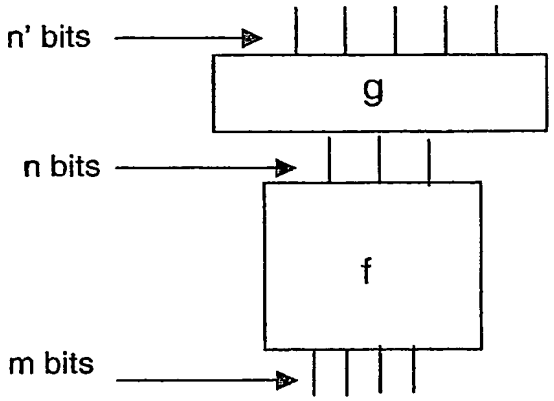


FIG.1a

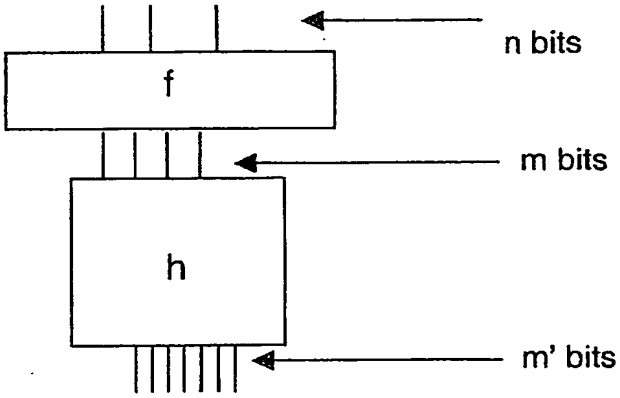


FIG.1b

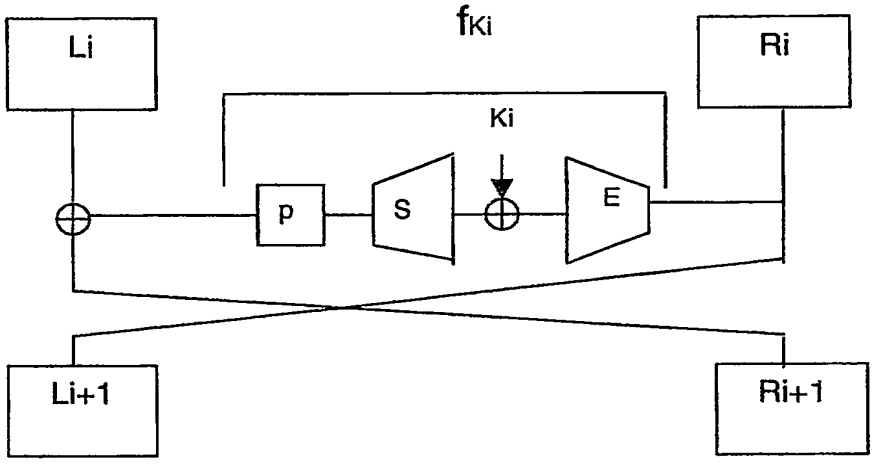
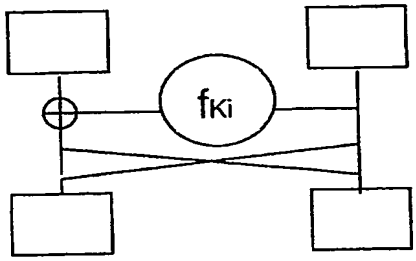


FIG.2

FIG.3a



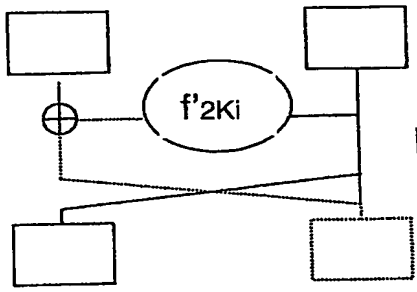
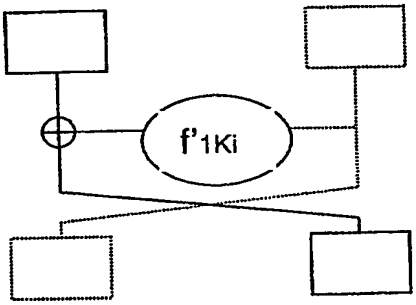


FIG.3b

FIG.3c



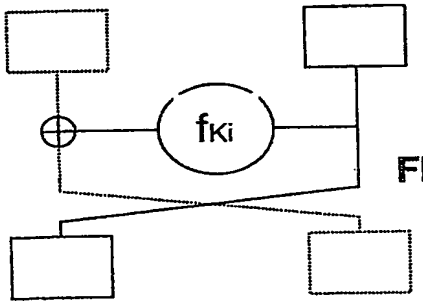
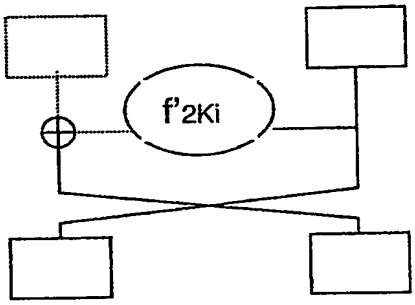


FIG.3d

FIG.3e



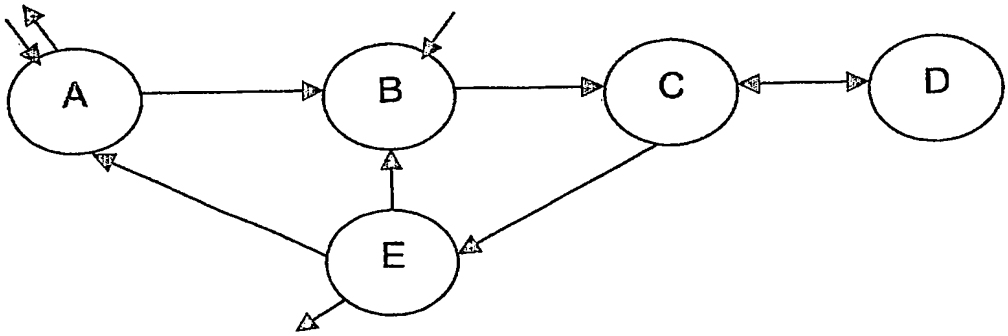


FIG.4

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'U[redacted]TÉ
Code de la propriété intellectuelle - Livre VI

N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

Vos références pour ce dossier *(facultatif)*	**FR 76.0728/PR**
N° D'ENREGISTREMENT NATIONAL	0202918

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de sécurisation d'un ensemble électronique de cryptographie à clè secrète

LE(S) DEMANDEUR(S) :

CP8
36 – 38 Rue de la Princesse -BP 45
78431 LOUVECIENNES CEDEX- FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		**Goubin**
Prénoms		**Louis**
Adresse	Rue	4 rue Mizon
	Code postal et ville	75015 PARIS - FRANCE
Société d'appartenance *(facultatif)*		
Nom		**Akkar**
Prénoms		**Mehdi-Laurent**
Adresse	Rue	17 rue Lafouge
	Code postal et ville	94250 GENTILLY – France
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

Louveciennes, le 6 mars 2002

Patricia RENAULT
Mandataire

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.